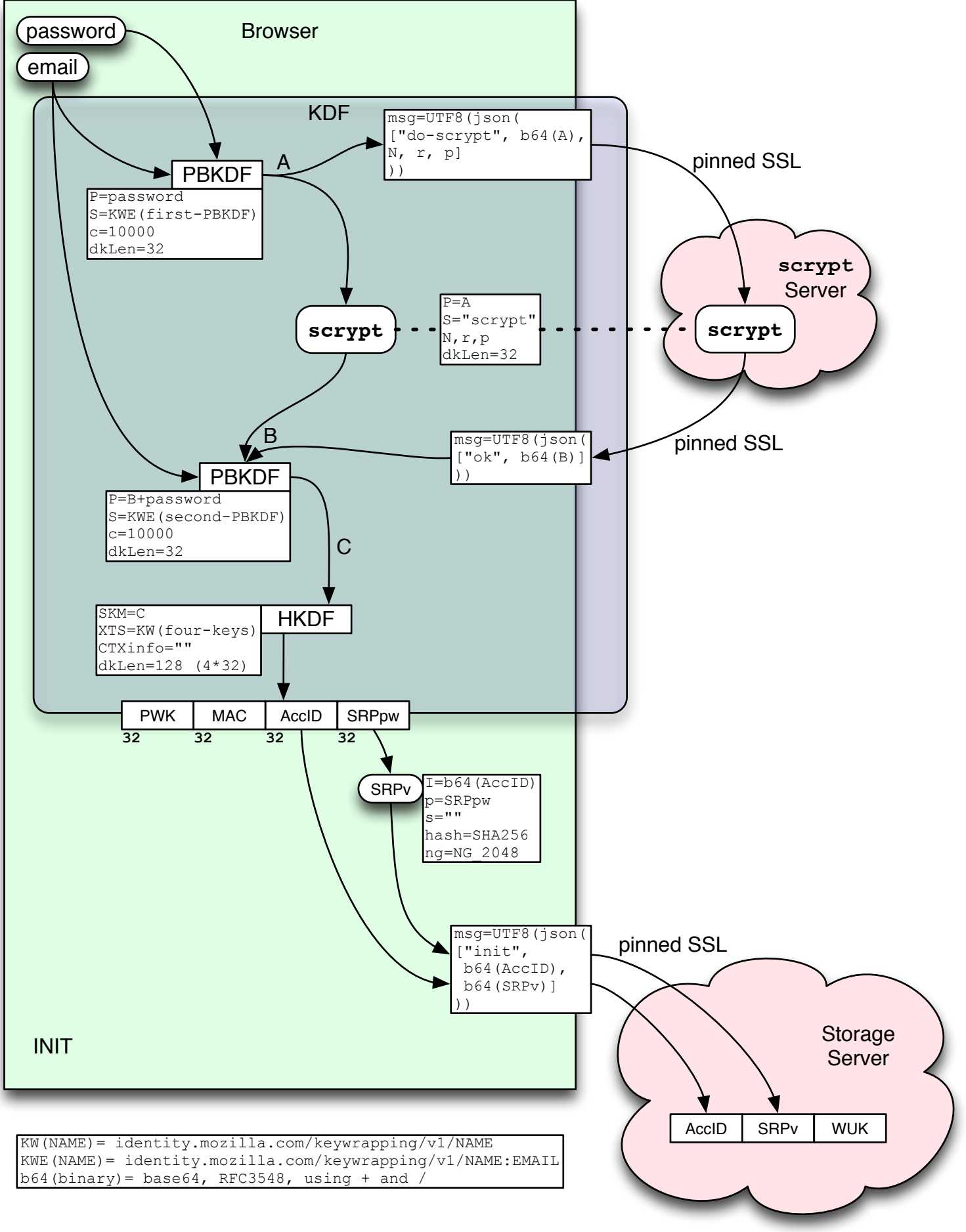
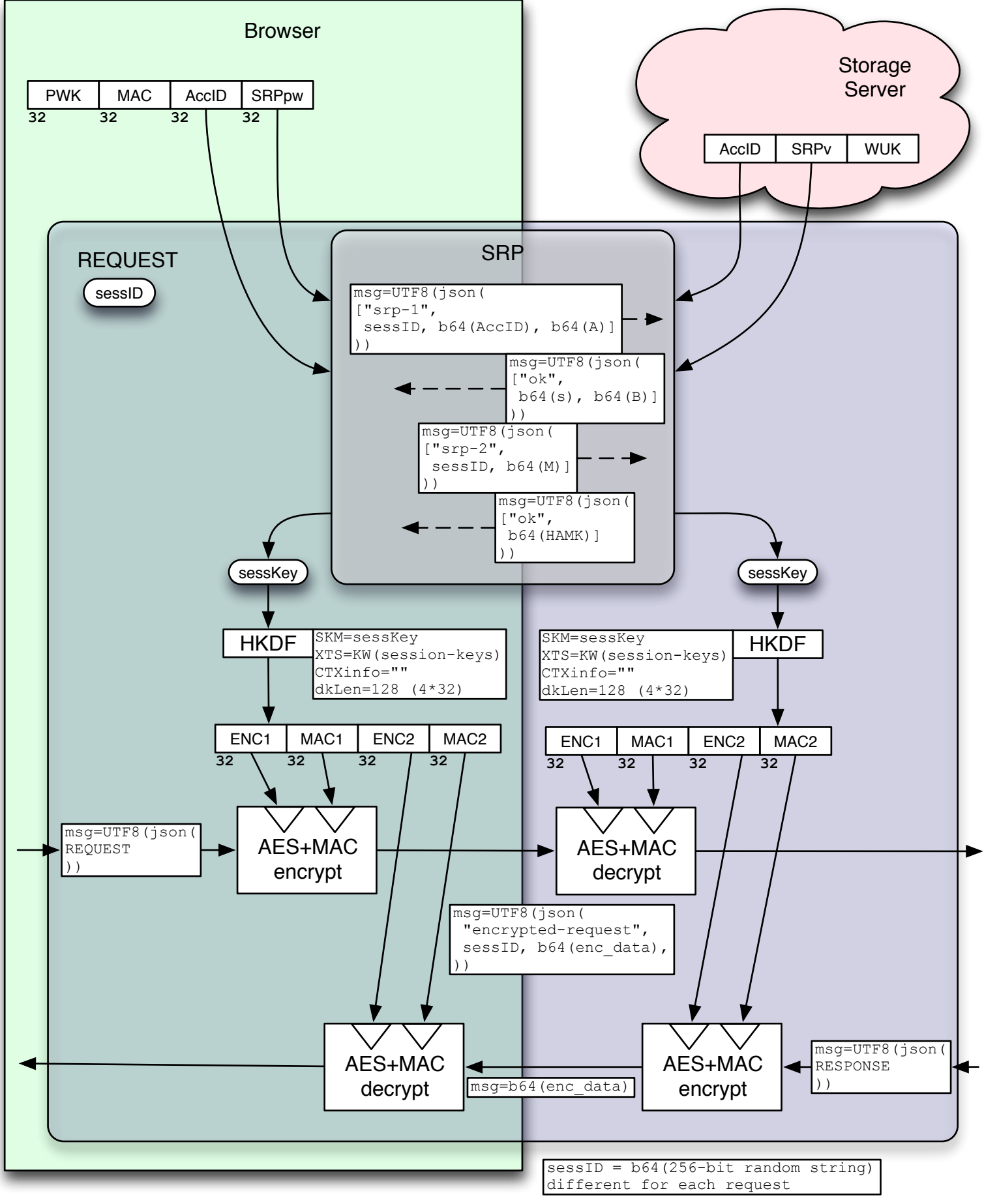
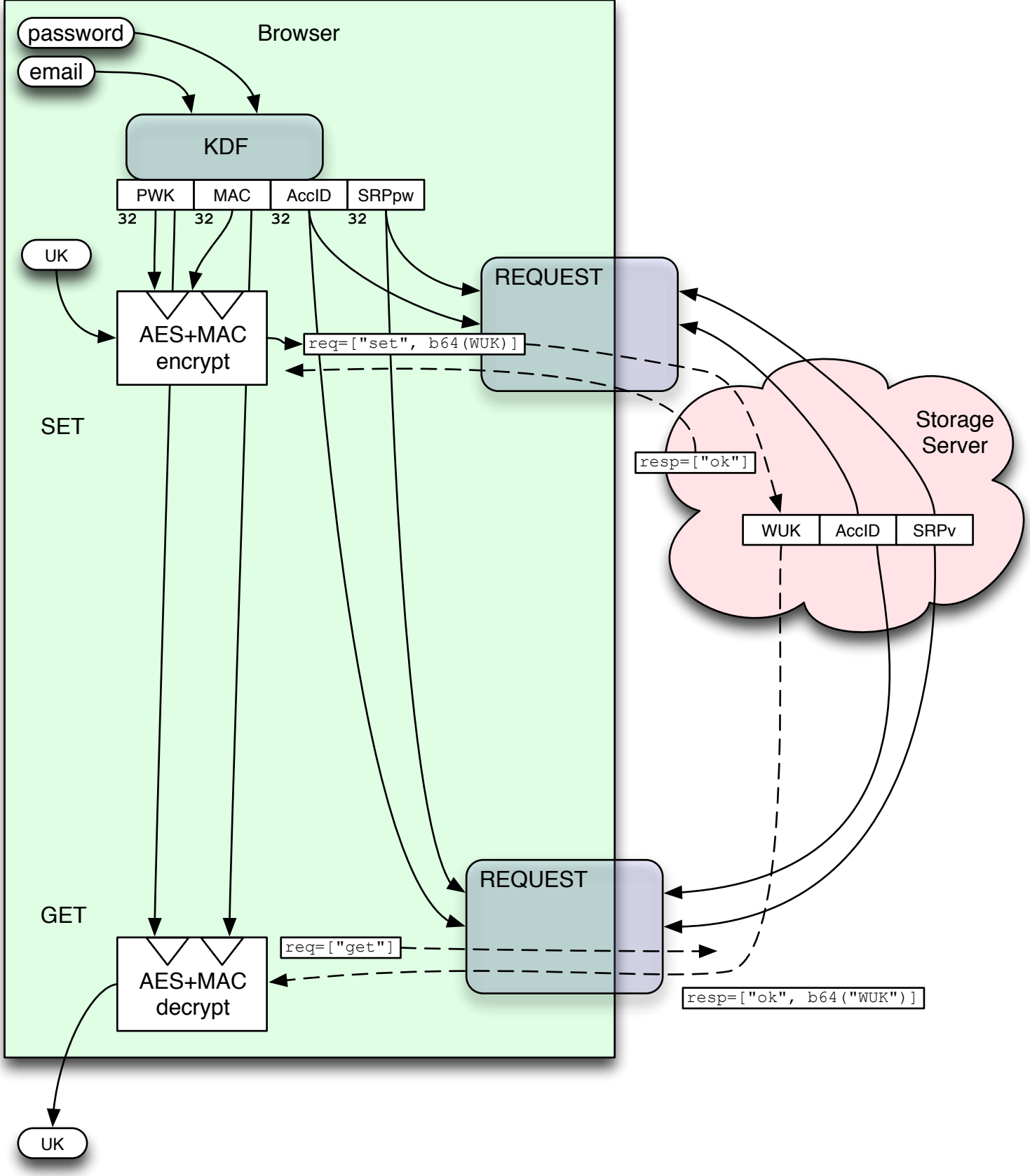
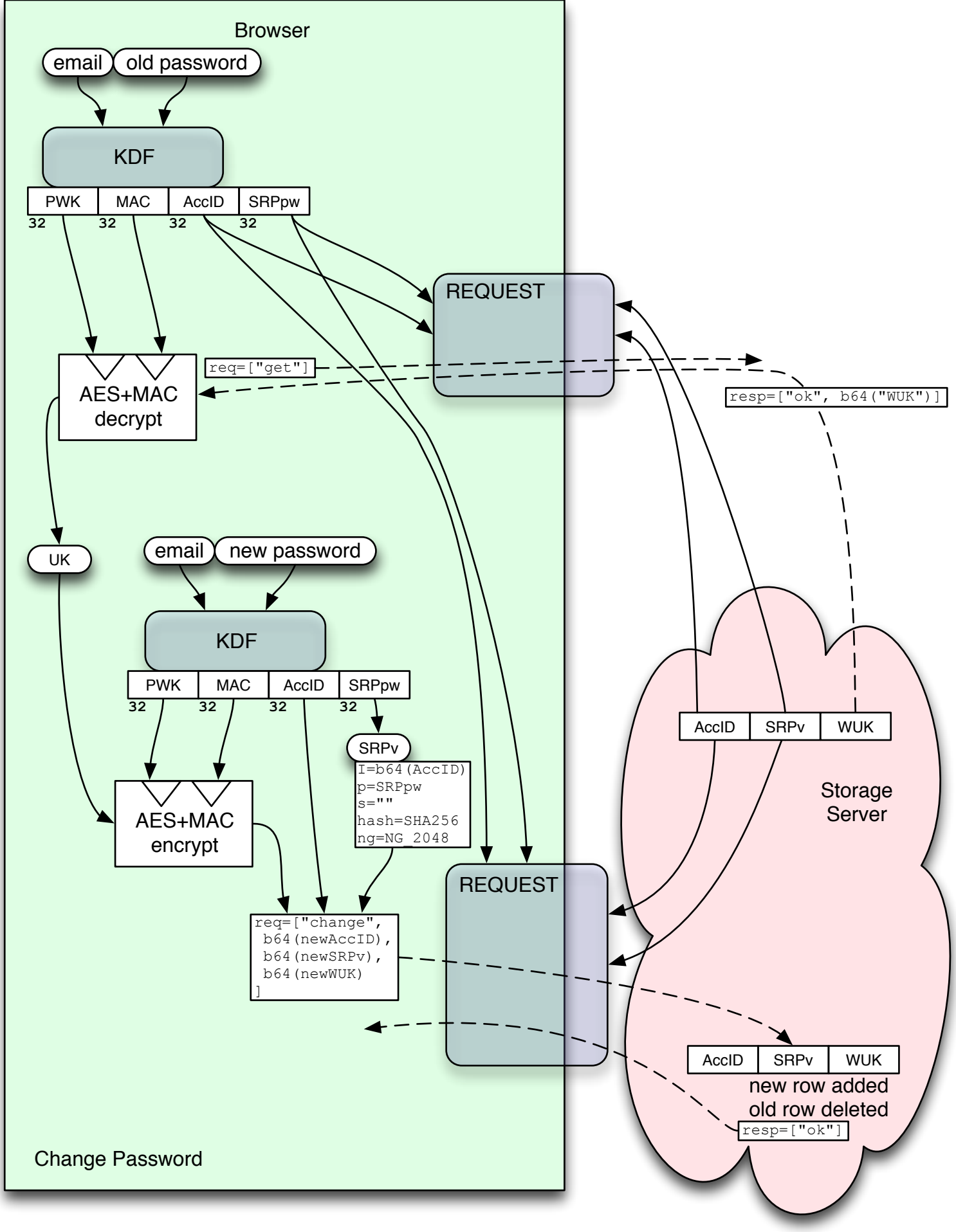

password
email
Browser
KDF
PBKDF
P=password
S=KWE(first-PBKDF)
c=10000
dkLen=32
A
msg=UTF8(json(
["do-scrypt", b64(A),
N, r, p]
))
pinned SSL
scrypt
Server
scrypt
P=A
S="scrypt"
N,r,p
dkLen=32
scrypt
B
msg=UTF8(json(
["ok", b64(B)]
))
pinned SSL
PBKDF
P=B+password
S=KWE(second-PBKDF)
c=10000
dkLen=32
C
SKM=C
XTS=KW(four-keys)
CTXinfo=""
dkLen=128 (4*32)
HKDF
PWK
MAC
AccID
SRPpw
32
32
32
32
SRPv
I=b64(AccID)
p=SRPpw
s=""
hash=SHA256
ng=NG_2048
msg=UTF8(json(
["init",
b64(AccID),
b64(SRPv)]
))
pinned SSL
INIT
Storage
Server
AccID
SRPv
WUK
KW(NAME)= identity.mozilla.com/keywrapping/v1/NAME
KWE(NAME)= identity.mozilla.com/keywrapping/v1/NAME:EMAIL
b64(binary)= base64, RFC3548, using + and /


Browser
PWK
MAC
AccID
SRPpw
32
32
32
32
Storage Server
AccID
SRPv
WUK
REQUEST
sessID
SRP
msg=UTF8(json(
["srp-1",
sessID, b64(AccID), b64(A)]
))
msg=UTF8(json(
["ok",
b64(s), b64(B)]
))
msg=UTF8(json(
["srp-2",
sessID, b64(M)]
))
msg=UTF8(json(
["ok",
b64(HAMK)]
))
sessKey
sessKey
HKDF
SKM=sessKey
XTS=KW(session-keys)
CTXinfo=""
dkLen=128 (4*32)
SKM=sessKey
XTS=KW(session-keys)
CTXinfo=""
dkLen=128 (4*32)
HKDF
ENC1
MAC1
ENC2
MAC2
32
32
32
32
ENC1
MAC1
ENC2
MAC2
32
32
32
32
msg=UTF8(json(
REQUEST
))
AES+MAC
encrypt
AES+MAC
decrypt
msg=UTF8(json(
"encrypted-request",
sessID, b64(enc_data),
))
AES+MAC
decrypt
msg=b64(enc_data)
AES+MAC
encrypt
msg=UTF8(json(
RESPONSE
))
sessID = b64(256-bit random string)
different for each request


password
email
Browser
KDF
PWK
MAC
AccID
SRPpw
32
32
32
32
UK
AES+MAC
encrypt
REQUEST
req=["set", b64(WUK)]
SET
Storage
Server
resp=["ok"]
WUK
AccID
SRPv
REQUEST
GET
req=["get"]
AES+MAC
decrypt
resp=["ok", b64("WUK")]
UK


Browser
email
old password
KDF
PWK
MAC
AccID
SRPpw
32
32
32
32
REQUEST
AES+MAC
decrypt
req=["get"]
resp=["ok", b64("WUK")]
UK
email
new password
KDF
PWK
MAC
AccID
SRPpw
32
32
32
32
SRPv
I=b64(AccID)
p=SRPpw
s=""
hash=SHA256
ng=NG_2048
AES+MAC
encrypt
REQUEST
req=["change",
b64(newAccID),
b64(newSRPv),
b64(newWUK)
]
AccID
SRPv
WUK
Storage
Server
AccID
SRPv
WUK
new row added
old row deleted
resp=["ok"]
Change Password